ARITHMETIC STRUCTURE IN SPARSE DIFFERENCE SETS

MARIAH HAMEL NEIL LYALL KATHERINE THOMPSON NATHAN WALTERS

Abstract. Using a slight modification of an argument of Croot, Ruzsa and Schoen we establish a quantitative result on the existence of a dilated copy of any given configuration of integer points in sparse difference sets. More precisely, given any configuration $\{v_1, \dots, v_\ell\}$ of vectors in $\mathbb{Z}^d$, we show that if $A \subset [1, N]^d$ with $|A|/N^d \geq CN^{-1/\ell}$, then there necessarily exists $r \neq 0$ such that $\{rv_1, \dots, rv_\ell\} \subseteq A - A$.

1. Introduction

Many familiar theorems in mathematics have as a common feature the phenomenon that the set of differences from a sufficiently large set contains non-trivial structure. In this paper we study instances of this phenomenon in the finite setting of subsets of $\{1, 2, \dots, N\}^d$. In this setting we are able obtain to quantitative structure theorems by adapting an argument of Croot, Ruzsa and Schoen [3].

1.1. Arithmetic progressions in sumsets.

A good measure of the amount of additive structure in a given finite set of integers is provided by the size of the longest arithmetic progression that the set contains.

In [3] Croot, Ruzsa and Schoen establish, using only simple combinatorial arguments, the following structural result along these very lines for the sumset

$$A + B := \{a + b : a \in A, b \in B\} \tag{1}$$

of two given sparse sets $A, B \subseteq [1, N] = \{1, 2, \dots, N\}$.

Theorem A (Croot, Ruzsa and Schoen [3]). *Let $A, B \subseteq [1, N]$ and $m \geq 3$ be an odd positive integer.*

If $|A||B|/N^2 \geq 6N^{-2/(m-1)}$, then $A + B$ contains an arithmetic progression of length at least m.

We remark that if $|A||B|/N^2 \geq (\log N)^{-1+\varepsilon}$, for any $\varepsilon > 0$, then the conclusion of Theorem A can in fact be strengthened significantly. Using Fourier analytic techniques Green [4], improving on previous work of Bourgain [2], proved the following

Theorem B (Green [4]). *Let $A, B \subseteq [1, N]$, then there exist absolute constants $0 < c < 1 < C$ such that if*

$$\frac{|A||B|}{N^2} \geq C\frac{(\log\log N)^2}{\log N}$$

then $A + B$ contains an arithmetic progression of length at least $\exp\Big(c\left(\frac{|A||B|}{N^2}\log N\right)^{1/2}\Big)$.

Ruzsa [10] has shown that for any $\varepsilon > 0$ and N sufficiently large, there exists a set $A \subseteq [1, N]$ with $|A|/N \geq 1/2 - \varepsilon$ whose sumset $A + A$ does not contain an arithmetic progression of length $\exp\big((\log N)^{2/3+\varepsilon}\big)$.

In this paper we give a slight simplification of the proof of Theorem A that appears in [3] and show how this can then be easily adapted to prove the natural higher dimensional generalization of Theorem A (as well as certain polynomial variants).

This work was carried out while all four authors were members of the *VIGRE Research Group in Arithmetic Combinatorics at the University of Georgia*. The first, third and fourth authors were partially supported by this NSF VIGRE grant. The second author was partially supported by NSF grant 0707099.

1.2. **Multi-dimensional configurations in sparse difference sets.** The main result of this paper is the following quantitative multi-dimensional Szemerédi theorem for sparse difference sets.

Theorem 1. *Given any collection $v_1, \dots, v_\ell$ of vectors in $\mathbb{Z}^d$ there exists a constant $C_{\ell,d} = C_{\ell,d}(v_1, \dots, v_\ell)$ such that the* difference set *of any set $A \subseteq [1,N]^d$ with*

$$|A|/N^d \geq C_{\ell,d} N^{-1/\ell}$$

will be guaranteed to contain some dilate of the original configuration $\{v_1, \dots, v_\ell\}$, that is to say that there will necessarily exist an integer $r > 0$ for which

$$\{rv_1, \dots, rv_\ell\} \subseteq A - A.$$

Remark 1. Since $A - A$ is symmetric it will also contain the reflection in the origin of this configuration, namely the configuration $\{-rv_1, \dots, -rv_\ell\}$.

A simple averaging argument (that we will make use of again and again) allows us to deduce, from Theorem 1, the following structural result for the sumset $A + B$ of two given sets $A, B \subseteq [1,N]^d$.

Corollary 1. *Let $v_1, \dots, v_\ell \in \mathbb{Z}^d$ and $A, B \subseteq [1,N]^d$. If $|A||B|/N^{2d} \geq 2^d C_{\ell,d} N^{-1/\ell}$, then there exists $r \neq 0$ and $t \in [2,2N]^d$ such that*

$$t \pm r \cdot \{v_1, \dots, v_\ell\} \subseteq A + B.$$

Proof. Since

$$\sum_{t \in [2,2N]^d} |B \cap (t - A)| = |A||B|$$

it follows that there exists $t \in [2,2N]^d$ such that if we set $D = B \cap (t - A)$, then

$$|D| \geq \frac{|A||B|}{(2N-1)^d}.$$

The result therefore follows immediately from Theorem 1 since $D - D + t \subseteq A + B$. □

Remark 2 (On the constant $C_{\ell,d}$ in Theorem 1 and Corollary 1). Given any collection $v_1, \dots, v_\ell$ of vectors in $\mathbb{Z}^d$ let s denote the size of the largest projection of these given vectors onto the coordinate axes. In other words we define

$$s = s(v_1, \dots, v_\ell) = \max_{1 \leq j \leq \ell} \|v_j\|_\infty = \max\{\, |\langle v_j, e_i \rangle| \,:\, 1 \leq j \leq \ell,\, 1 \leq i \leq d \}, \tag{2}$$

where $\{e_i\}_{1 \leq i \leq d}$ denotes the standard basis vectors for $\mathbb{Z}^d$.

It is clear that in order to obtain a non-trivial conclusion in Theorem 1 and Corollary 1 we must have $r \in [1, N/s]$, and in particular $N \geq s$ (a fact that will be forced on us by the choice of constant $C_{\ell,d}$).

In the proof of Theorem 1, which we present in Section 4, we will see that we can in fact take

$$C_{\ell,d} := \Big(2s \prod_{i=1}^{d} \prod_{j=1}^{\ell} \Big(1 + \frac{|\langle v_j, e_i \rangle|}{s}\Big)\Big)^{1/\ell} \leq 2^d (2s)^{1/\ell}. \tag{3}$$

It follows that we are able to recover Theorem A, the structural result for sparse sumsets of Croot, Ruzsa and Schoen, with only marginally weaker bounds (the constant 6 replaced with 8) as a special case of Corollary 1, namely the special case $d = 1$ with $v_j = j$.

Finally, it is also easy to see that for specific (and interesting) choices of vectors $v_1, \dots, v_\ell \in \mathbb{Z}^d$ the true value of $C_{\ell,d}$ is significantly smaller than the trivial upper bound of $2^d(2s)^{1/\ell}$. For example, in the case when $\ell = d$ and $v_j = e_j$ (a d-dimensional corner), we have $C_{\ell,d} \leq 2^{1+1/\ell}$.

1.3. **Outline of the paper.** In Section 2 we present a proof of Theorem 1 in the special case when $d = 1$ with $v_j = j$. As a corollary of this result (and some known quantitative results on polynomial patterns in difference sets) we give quantitative bounds on the size of a set $A \subseteq [1, N]$ that will ensure that its difference set contains a long arithmetic progression whose common difference is a perfect square.

In Section 3 we formulate a polynomial generalization of Theorem 1, namely Theorem 5, and present a proof of this result in a special case (Theorem 3).

Finally, in Section 4 we prove Theorem 1 and sketch the proof of Theorem 5.

2. Arithmetic progressions in sparse difference sets

2.1. **A special case of Theorem 1.** Although the following result can be extracted from Croot, Ruzsa and Schoen [3] we feel that the argument below is perhaps slightly simpler and easier to generalize.

Theorem 2 (A special case of Theorem 1)**.** *Let $A \subseteq [1, N]$ and $m \geq 3$ be an odd positive integer.*

If $|A|/N \geq 4N^{-2/(m-1)}$, then $A - A$ contains an arithmetic progression of length at least m.

Proof of Theorem 2. Let $m = 2\ell + 1$. For each $w = (w_1, \dots, w_\ell) \in \mathbb{Z}^\ell$ we define[1]

$$\mathcal{R}_w = \{r \in [1, N/\ell] \,:\, jr + w_j \in A \ (1 \leq j \leq \ell)\}$$

and note that if, for some $w \in \mathbb{Z}^\ell$, there exist $r', r'' \in \mathcal{R}_w$ with $r' \neq r''$, then it follows immediately that

$$j(r' - r'') \in A - A$$

for each $1 \leq j \leq \ell$ and hence, utilizing the fact that $A - A$ is symmetric, that the difference set $A - A$ contains an arithmetic progression of length $2\ell + 1$.

It therefore suffices to establish the existence of a $w \in \mathbb{Z}^\ell$ such that $|\mathcal{R}_w| \geq 2$. In order to do this we (naturally) restrict our attention to those w for which $\mathcal{R}_w$ has at least a chance of being non-empty, namely

$$\mathcal{W} = \{w \in \mathbb{Z}^\ell \,:\, 1 - jN/\ell \leq w_j \leq N - 1 \ (1 \leq j \leq \ell)\},$$

and note that

$$|\mathcal{W}| \leq N^\ell \prod_{j=1}^{\ell} (1 + j/\ell) \leq 2^\ell N^\ell.$$

Since the average

$$\frac{1}{|\mathcal{W}|} \sum_{w \in \mathcal{W}} |\mathcal{R}_w| = \frac{1}{|\mathcal{W}|} \sum_{w \in \mathcal{W}} \sum_{r=1}^{N/\ell} \prod_{j=1}^{\ell} 1_A(jr + w_j) = \frac{1}{|\mathcal{W}|} |A|^\ell \frac{N}{\ell}$$

it follows that there must exist a $w \in \mathcal{W}$ such that

$$|\mathcal{R}_w| \geq \left(\frac{|A|}{N}\right)^\ell \frac{N}{\ell 2^\ell}$$

and consequently, for this choice of w, that the set $\mathcal{R}_w$ will contain at least 2 elements provided

$$\frac{|A|}{N} \geq C_\ell \frac{1}{N^{1/\ell}}$$

where $C_\ell = 2(2\ell)^{1/\ell}$. It is an easy (calculus) exercise to finally show that $2 \leq C_\ell \leq 4$. □

It is clear that the arguments presented above are flexible enough to be applied almost verbatim to more general situations and at this point the reader is encouraged to prove Theorem 1 for herself (the details can be found in Section 4).

We now turn our attentions to the problem of finding polynomial configurations in difference sets.

[1] Of course N/ℓ need not be an integer, however here, and in the remainder of this article, we will make the slight (but convenient) abuse of notation of identifying $[1, x]$ with $[1, \lfloor x \rfloor]$ for any given positive real number x.

2.2. **Some remarks on polynomial configurations in difference sets.** The following result, a quantitative polynomial Szemerédi theorem for difference sets, can be established by a careful application of standard Fourier analytic (circle method) techniques, see [6] and [7].

Theorem C (Lyall and Magyar [7]). *Let $P_1, \dots, P_\ell \in \mathbb{Z}[r]$ with each $P_j(0) = 0$ and $k = \max_j \deg P_j \geq 2$.*

There exists an absolute constant $C = C(P_1, \dots, P_\ell)$ such that for any $A \subseteq [1, N]$ with

$$\frac{|A|}{N} \geq C \left(\frac{(\log\log N)^2}{\log N} \right)^{1/\ell(k-1)}$$

there necessarily exist $r \neq 0$ such that

$$\{P_1(r), \dots, P_\ell(r)\} \subseteq A - A.$$

In the case of a single polynomial ($\ell = 1$), this result was also obtained by Lucier [5] and, to the best of our knowledge, constitutes the best bounds that are currently known for arbitrary polynomials with integer coefficients and zero constant term. However, using some rather involved Fourier arguments, Pintz, Steiger and Szemerédi in [8] were able to establish the following impressive result for square differences.

Theorem D (Pintz, Steiger and Szemerédi [8]). *Let $A \subseteq [1, N]$ and $m \geq 3$ be a positive integer. If*

$$\frac{|A|}{N} \geq C \left(\frac{1}{\log N} \right)^{c \log\log\log\log N}$$

then there necessarily exist $r \neq 0$ such that $r^2 \in A - A$.

We note that it is conjectured that for any $\epsilon > 0$ and N sufficiently large there exists a set $A \subseteq [1, N]$ with $|A| \geq N^{1-\epsilon}$ that contains no square differences. Ruzsa [9] has demonstrated this for $\epsilon = 0.267$.

Arguing as in the proof of Theorem 2 we can deduce, from Theorem D, the following result pertaining to arithmetic progressions with square differences.

Corollary 2. *Let $A \subseteq [1, N]$ and $m \geq 3$ be a positive integer. If*

$$\frac{|A|}{N} \geq C' \left(\frac{1}{\log N} \right)^{2c' \log\log\log\log N/(m-1)}$$

then $A - A$ contains an arithmetic progression of length at least m with common difference r^2 (with $r \in \mathbb{N}$).

Proof. Let $m = 2\ell + 1$. For each $w = (w_1, \dots, w_\ell) \in \mathbb{Z}^\ell$ we again define

$$\mathcal{R}_w = \{r \in [1, N/\ell] : jr + w_j \in A \ (1 \leq j \leq \ell)\}.$$

It follows from Theorem D that if, for some $w \in \mathbb{Z}^\ell$ we have

$$\frac{|R_w|}{N/\ell} \geq C \left(\frac{1}{\log N/\ell} \right)^{c \log\log\log\log(N/\ell)} \tag{4}$$

then there will necessarily exist $r', r'' \in \mathcal{R}_w$ and $r \neq 0$ such that $r' - r'' = r^2$ and consequently also that

$$jr^2 \in A - A$$

for each $1 \leq j \leq \ell$. Utilizing the fact that $A - A$ is symmetric, it then follows that the difference set $A - A$ contains an arithmetic progression of length $2\ell + 1$ with a square common difference.

It therefore suffices to establish a condition on the set A guaranteeing that estimate (4) will hold. We saw, in the proof of Theorem 2 above, that there exists $w = (w_1, \dots, w_\ell) \in \mathbb{Z}^\ell$ such that

$$\frac{|R_w|}{N/\ell} \geq \left(\frac{|A|}{N} \right)^\ell \frac{1}{2^\ell}.$$

Hence, inequality (4) will hold provided

$$\frac{|A|}{N} \geq 2C^{1/\ell}\left(\frac{1}{\log N/\ell}\right)^{c\log\log\log\log(N/\ell)/\ell}$$

and the result follows. □

The methods of Pintz, Steiger and Szemerédi were later extended by Balog, Pelikán, Pintz and Szemerédi [1] to obtain Theorem D (with the same bounds, but with the constant C now depending on k), and hence also Corollary 2, for kth power differences. However, as we mentioned above, these impressive bounds have yet to be established for arbitrary polynomials with integer coefficients and zero constant term.

3. A polynomial generalization of Theorem 1

3.1. **A special case of Theorems 4 and 5.** Before stating our polynomial generalization of Theorem 1, namely Theorem 5 (which contains as a special case a weak variant of Theorem C for sparse difference sets), we present the following very special case. It is our hope that working through this special case will help motivate the ultimate formulation of Theorem 5.

Theorem 3 (A special case of Theorems 4 and 5)**.** *Let $P(r) = a_k r^k + \cdots + a_1 r + a_0$ with each $a_j \in \mathbb{Z}$ and $a_k > 0$. If N is sufficiently large and $A \subseteq [1, N]$ with*

$$|A|/N \geq (4a_k^{1/k})N^{-1/k}$$

then there exist $r', r'' \in \mathbb{N}$ with $r' \neq r''$ such that

$$P(r') - P(r'') \in A - A.$$

Note that a conclusion of the form $P(r) \in A-A$ for such sparse sets is forbidden, see the remark proceeding Theorem D concerning partial progress towards a conjecture of Ruzsa.

Proof. It suffices to establish the existence of a $w \in \mathbb{Z}$ such that $|\mathcal{R}_w| \geq 2$ where

$$\mathcal{R}_w = \{r \in [1, N_0] \,:\, P(r) + w \in A\}$$

with $N_0 = (N/a_k)^{1/k}$. We define $\mathcal{W}$ to be the *smallest* collection of $w \in \mathbb{Z}$ for which

$$P(r) + \mathcal{W} \supseteq [1, N]$$

for all $r \in [1, N_0]$. If N is sufficiently large (depending on the coefficients of P) it follows that

$$\max_{r\in[1,N_0]} |P(r)| \leq P(N_0) \leq 2N$$

and hence that

$$\mathcal{W} \subseteq \{w \in \mathbb{Z} \,:\, 1 - P(N_0) \leq w \leq P(N_0) - 1\}$$

from which we can conclude that

$$|\mathcal{W}| \leq 4N.$$

Remark 3. If $P(r) > 0$ on $[1, N_0]$, then we could conclude, as in the proof of Theorem 2, that in fact $|\mathcal{W}| \leq 2N$ (provided that N is large enough). In the further special case when $P(r) = a_k r^k$ we note that one can drop the "let N be sufficiently large" assumption in the statement of the theorem.

Since the average

$$\frac{1}{|\mathcal{W}|}\sum_{w\in\mathcal{W}} |\mathcal{R}_w| = \frac{1}{|\mathcal{W}|}\sum_{w\in\mathcal{W}}\sum_{r=1}^{N_0} 1_A(P(r)+w) \geq \frac{|A|N_0}{4N}$$

for N sufficiently large, it follows that if

$$|A|/N \geq (4a_k^{1/k})N^{-1/k}$$

and N is sufficiently large, then there will necessarily exist $w \in \mathcal{W}$ for which $|\mathcal{R}_w| \geq 2$. □

3.2. **A polynomial variant of Theorem 1.** Let $\{v_1, \dots, v_\ell\}$ be a fixed configuration of vectors in $\mathbb{Z}^d$. Given polynomials $P_1, \dots, P_\ell \in \mathbb{Z}[r]$ with $\max_{1\leq j\leq \ell} \deg P_j \leq k$, our methods allow us to establish the following *non-isotropic* generalization of Theorem 1.

Theorem 4. *If $A \subseteq [1,N]^d$ with $|A|/N^d \geq CN^{-1/\ell k}$, for some constant C, then there exist $r', r'' \in \mathbb{N}$ with $r' \neq r''$ such that*

$$\{(P_1(r') - P_1(r''))\, v_1, \dots, (P_\ell(r') - P_\ell(r''))\, v_\ell\} \subseteq A - A.$$

Since, for each $1 \leq j \leq \ell$, we can write

$$(P_j(r') - P_j(r''))\, v_j = \sum_{i=1}^{d} (Q_{ij}(r') - Q_{ij}(r''))\, e_i$$

where $Q_{ij}(r) := P_j(r)\langle v_j, e_i\rangle$ we see that Theorem 4 is a special case of the following more general result.

Theorem 5. *Let $\mathcal{Q} = \{Q_{ij}\}_{\substack{1\leq i\leq d\\ 1\leq j\leq \ell}}$ be a fixed collection of ℓd polynomials in $\mathbb{Z}[r]$ and $k = \max_{Q_{ij}\in\mathcal{Q}} \deg Q_{ij}$, then there exists a constant $C_{\ell,d,k} = C_{\ell,d,k}(\mathcal{Q})$ such that if N is sufficiently large and $A \subseteq [1,N]^d$ with*

$$|A|/N^d \geq C_{\ell,d,k} N^{-1/\ell k}$$

then there exists $r', r'' \in \mathbb{N}$ with $r' \neq r''$ such that

$$\sum_{i=1}^{d} (Q_{ij}(r') - Q_{ij}(r''))\, e_i \in A - A.$$

Remark 4 (on the constant $C_{\ell,d,k}$ in Theorem 5). If we now let t denote the absolute value of the largest leading coefficient of the polynomials that have the largest degree, namely

$$t = \max_{Q_{ij}\in\mathcal{Q}} \lim_{r\to\infty} |Q_{ij}(r)|/r^k \tag{5}$$

then, as we shall see in the proof below, we will be able take

$$C_{\ell,d,k} = 4^d (2t^{1/k})^{1/\ell}$$

in general and replace the 4 with 2 in the special case where the Q_{ij} take only positive values on $\mathbb{N}$.

Note that we *exactly* recover Theorem 1 (with the same constant) as a special case of Theorem 5, namely the special case where $Q_{ij}(r) = r\langle v_j, e_i\rangle$, since in this case we can drop the "let N be sufficiently large" assumption (see Remark 3 in the proof of Theorem 3), we leave this observation for the reader to verify.

4. Proof of Theorem 1 and Theorem 5

4.1. **Proof of Theorem 1.** Let s be defined by formula (2). For each $w = (w_1, \dots, w_\ell) \in (\mathbb{Z}^d)^\ell$ we define

$$\mathcal{R}_w = \{r \in [1, N/s] \,:\, rv_j + w_j \in A \ (1 \leq j \leq \ell)\}$$

and $\mathcal{W}$ to be the *smallest* collection of $w = (w_1, \dots, w_\ell) \in (\mathbb{Z}^d)^\ell$ for which

$$\{rv_j + w_j \,:\, w \in \mathcal{W}\} \supseteq [1,N]^d$$

for all $1 \leq j \leq \ell$ and $r \in [1, N/s]$.

As in the proof of Theorem 2 it will suffice to establish the existence of a $w \in \mathcal{W}$ such that $|\mathcal{R}_w| \geq 2$. The fact that this happens whenever

$$\left(\frac{|A|}{N^d}\right)^\ell \geq \frac{2s}{N} \prod_{i=1}^{d} \prod_{j=1}^{\ell} \Big(1 + \frac{|\langle v_j, e_i\rangle|}{s}\Big)$$

follows immediately from the observation that the average

$$\frac{1}{|\mathcal{W}|}\sum_{w\in\mathcal{W}}|\mathcal{R}_w| = \frac{1}{|\mathcal{W}|}\sum_{w\in\mathcal{W}}\sum_{r=1}^{N/s}\prod_{j=1}^{\ell}1_A(rv_j+w_j) = \frac{1}{|\mathcal{W}|}|A|^\ell\frac{N}{s}$$

and the (easily verified) fact that

$$|\mathcal{W}| \le N^{d\ell}\prod_{i=1}^{d}\prod_{j=1}^{\ell}\Big(1+\frac{|\langle v_j,e_i\rangle|}{s}\Big).$$

4.2. **Proof of Theorem 5.** Let t be defined by formula (5). For each $w=(w_1,\dots,w_\ell)\in(\mathbb{Z}^d)^\ell$ we define

$$\mathcal{R}_w = \Big\{r\in[1,N_0]\,:\,w_j+\sum_{i=1}^{d}Q_{ij}(r)e_i\in A\ (1\le j\le\ell)\Big\},$$

with $N_0=(N/t)^{1/k}$. Since, for N sufficiently large (depending on the coefficients of Q_{ij}),

$$\max_{r\in[1,N_0]}|Q_{ij}(r)| \le |Q_{ij}(N_0)| \le 2N$$

for all $1\le j\le\ell$, we will restrict our attention to those w that are contained in the set

$$\mathcal{W} = \{w\in(\mathbb{Z}^d)^\ell\,:\,|\langle w_j,e_i\rangle|\le 2N-1\ (1\le j\le\ell,\,1\le i\le d)\},$$

and note that $|\mathcal{W}|\le(4N)^{\ell d}$ provided that N is sufficiently large. Since the average

$$\frac{1}{|\mathcal{W}|}\sum_{w\in\mathcal{W}}|\mathcal{R}_w| = \frac{1}{|\mathcal{W}|}\sum_{w\in\mathcal{W}}\sum_{r=1}^{N_0}\prod_{j=1}^{\ell}1_A\Big(w_j+\sum_{i=1}^{d}Q_{ij}(r)e_i\Big) \ge \left(\frac{|A|}{N^d}\right)^\ell\frac{N_0}{4^{\ell d}}$$

for N sufficiently large, it follows that there will necessarily exist $w\in\mathcal{W}$ for which $|\mathcal{R}_w|\ge 2$ provided that

$$|A|/N^d \ge (2^{1/\ell}4^d t^{1/\ell k})N^{-1/\ell k}$$

and N is sufficiently large.

References

[1] A. Balog, J. Pelikán, J. Pintz, E. Szemerédi, *Difference sets without κ-th powers*, Acta Math. Hungar. 65 (1994), 165-187.

[2] J. Bourgain, *On Arithmetic Progressions in Sums of Sets of Integers*, A tribute to Paul Erdős, 105-109, Cambridge University Press, Cambridge, 1990.

[3] E. Croot, I. Ruzsa, T. Schoen, *Long arithmetic progressions in sparse sumsets*, Integers: The Electronic Journal of Combinatorial Number Theory, 7(2) (2007), #A10. 2005.

[4] B. Green, *Arithmetic Progressions in Sumsets*, Geom. Funct. Anal. (2002), 584-597.

[5] J. Lucier, *Intersective sets given by a polynomial*, Acta Arith. 123 (2006), no. 1, 57-95.

[6] N. Lyall and Á. Magyar, *Polynomial configurations in difference sets*, J. Num. Theory, v. 129/2, pp. 439-450, 2009.

[7] N. Lyall and Á. Magyar, *Polynomial configurations in difference sets (revised version)*, `arxiv.org/abs/0903.4504`.

[8] J. Pintz, W. L. Steiger, E. Szemerédi, *On sets of natural numbers whose difference set contains no squares*, J. London Math. Soc. 37 (1988), 219-231.

[9] I. Z. Ruzsa, *Difference sets without squares*, Period. Math. Hungar. 15 (1984), 205-209.

[10] I. Z. Ruzsa, *Arithmetic Progressions in Sumsets*, Acta. Arith. (1991), no. 2, 191-202.

Department of Mathematics, The University of Georgia, Athens, GA 30602, USA

E-mail address: `mhamel@math.uga.edu, lyall@math.uga.edu, thompson@math.uga.edu, nwalters@math.uga.edu`